

Kapittel 1:

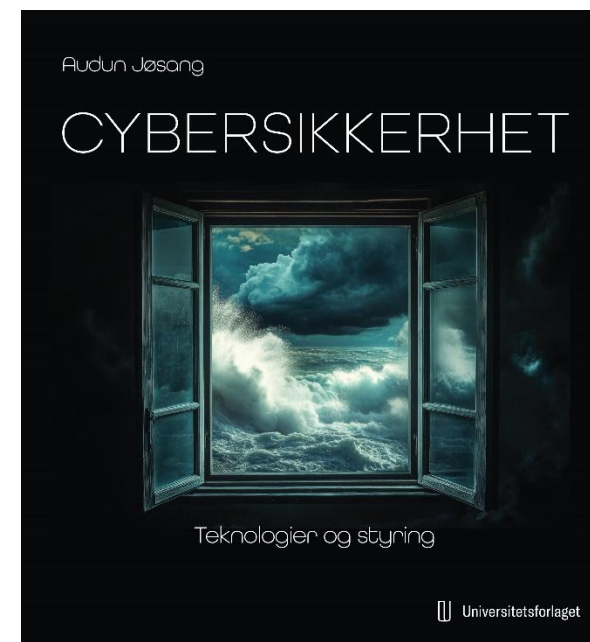
Begreper om cybersikkerhet

Cybersikkerhet: Teknologier og styring

Audun Jøsang

3. utg. 2025

Universitetsforlaget



Sikkerhet er beskyttelse av verdier mot skade

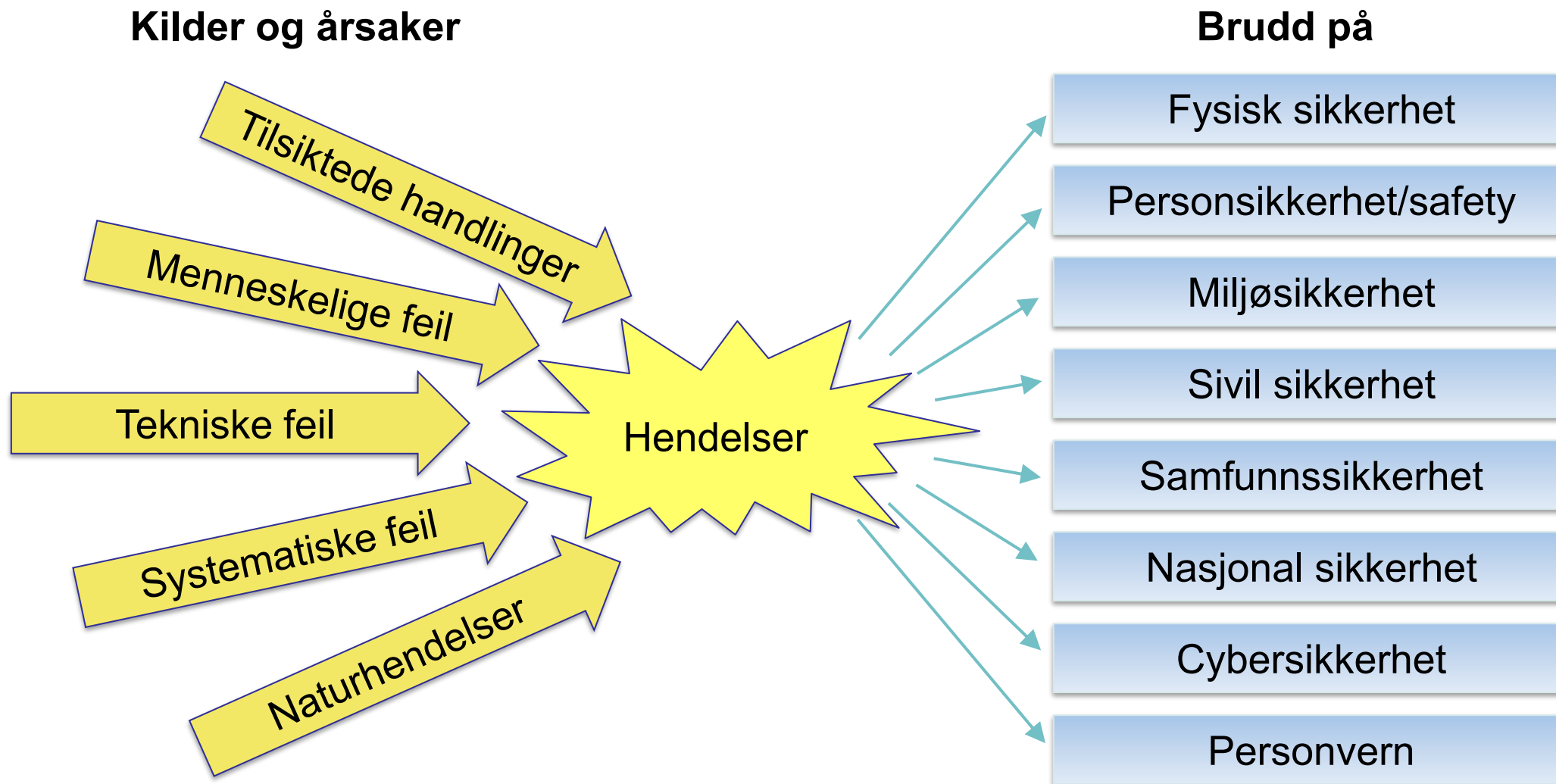
Eiendom Infrastruktur Demokrati Lov og orden Liv og helse Miljø Digitale verdier Persondata



- **Fysisk sikkerhet:** hindre innbrudd, tyveri og tukling med utstyr
- **Samfunnssikkerhet:** opprettholde funksjonalitet i kritiske infrastrukturer
- **Nasjonal sikkerhet:** demokrati, politisk stabilitet, territorial integritet
- **Sivil sikkerhet og rettssikkerhet:** opprettholdelse av lov og orden
- **Personsikkerhet / trygghet / safety:** beskyttelse av liv og helse
- **Miljø sikkerhet:** hindre forurensing og fremmede arter
- **Cybersikkerhet:** beskyttelse av digitale verdier
- **Personvern:** følge prinsipper for innhenting, lagring, behandling og deling av personopplysninger

Usikkerhet er mangel på beskyttelse av verdier mot skade, som antonym til sikkerhet.

Ulike kilder til brudd på sikkerhet



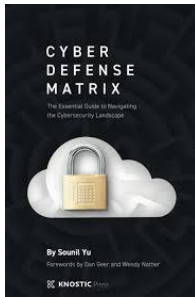
Hva er cybersikkerhet ?



- *Cybersikkerhet* er beskyttelse av *digitale verdier* mot skade. Det inkluderer beredskap for håndtering av hendelser og gjenoppretting når skade skjer.
- Hvilke kategorier av digital verdier skal beskyttes?
 - Cyberforsvarsmatrisen definerer digitale verdier som: ENHETER, APPER, NETTVERK, DATA, og BRUKERE. «Digitale verdier» kalles også «digitale eiendeler».
- Hvordan kan digitale verdier skades?
 - Brudd på et eller flere av sikkerhetsmålene Konfidensialitet, Integritet og Tilgjengelighet (KIT)
- Dekker både tilsiktet og utilsiktet skade
 - Trusselaktører kan være mennesker eller naturlige hendelser
 - Mennesker kan gjøre skade både tilsiktet og utilsiktet
- Definisjon av informasjonssikkerhet:
 - ***Beskyttelse av informasjonens Konfidensialitet, Integritet og Tilgjengelighet.***
I tillegg kan andre egenskaper, f.eks. autentisitet, sporbarhet, ubenektelighet og pålitelighet omfattes. (ISO/IEC 27000:2018)

Digitale verdier (se cyberforsvarsmatrisen, kap.18)

“Digitale verdier” kalles også “digitale eiendeler”



- ENHETER er maskinvare og standard installert programvaren som OS.
 - Fastvare, operativsystemer og standardapplikasjoner fra leverandører
 - Skill mellom ENHETER basert på hvem som eier enheten, for eksempel organisasjon, ansatte (BYOD) eller skyleverandører.
 - Nettverksenheter som svitsjer og rutere tilhører også denne klassen.
- APPER er applikasjoner og prosesser spesielt utviklet av eller for virksomheten.
 - APP-er produserer vanligvis tjenestene og produktene som leverer organisasjonens verdi og forretningsfunksjoner. Derfor er kontinuiteten og integriteten til APPS vanligvis kritisk.
- NETTVERK er kommunikasjonskanaler, rutere, protokoller og brannmurfiltreringer.
 - Konfigurasjon av nettverksenheter som DNS (Domain Name System), AS (Autonomous Systems) og PKI (Public Key Infrastructure), og som gir ruting, filtrering og VPN
- DATA er forretningsdata, som er lagret, som overføres eller brukes av verdiene over.
- BRUKERE er personene og AI-agentene, med ID-er og autentikatorer.
 - En AI-agent kan kanskje betraktes som en enhet, men hvis den har egenskapene til en bruker med sin egen ID, autentiseringslegitimasjon, tilgangsautorisasjoner og intelligente beslutninger.

Kjært barn har mange navn



- **Informasjonssikkerhet:** generelt begrep, dekker f.eks. også beskyttelse av informasjon på papir, populært fra 1970-tallet. Direkte oversettelse av «information security» som er nedfelt i en rekke internasjonale standarder og rammeverk.
- **Datasikkerhet:** (eng. Computer Security) kan tolkes som beskyttelse av data, men det betyr egentlig beskyttelse av datamaskiner, populært fra 1980-tallet.
- **IT- og IKT-sikkerhet:** tolkes som sikkerhet i IT/IKT-systemer, populært fra 1990-tallet.
- **Cybersikkerhet:** tolkes ofte som sikkerhet for alt som har å gjøre med Internett og som er koblet til Internett, populært fra 2010-tallet.
- **Digital sikkerhet:** skapt av norske myndigheter i 2019, med hensikt å være et samlebegrep for alle begrepene ovenfor, rimer godt med «digitalisering» og ser ut til å bli populært fremover.

Alle disse begrepene betyr det samme !

- **Sikring:** I noen sektorer (f.eks. olje og gass) der «sikkerhet» er ensbetydende med «safety» benyttes «sikring» i betydning av «security».

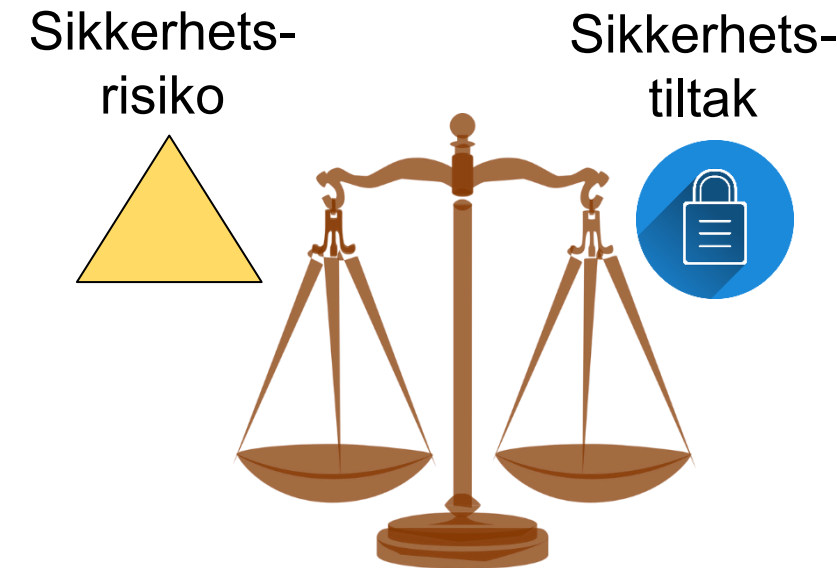
Kilder til krav om cybersikkerhet

- **God praksis:** Krav om adekvat sikkerhet i forretningsprosesser i henhold til vanlig god praksis og forvaltning.
 - Vanlig god praksis setter f.eks. krav om brukerautentisering og tilgangskontroll.
 - Veiledere for god praksis er f.eks. NSMs grunnprinsipper, NISTs CSF, og CIS controls (kap.18)
 - **Risikovurdering:** Krav om å begrense sikkerhetsrisiko til et forsvarlig nivå.
 - Tiltak identifiseres gjennom risikovurdering, f.eks. krav om 2-faktorautentisering.
 - Pentesting (enkel form for risikovurdering) avdekker sikkerhetssårbarheter som må fjernes.
 - **Regelverk:** Juridiske, lovbestemte, regulatoriske, bransje- og kontraktsmessige krav til informasjonssikkerhet, f.eks.:
 - Sikkerhetsloven setter krav om sikkerhet for grunnleggende nasjonale funksjoner.
 - Lov om digital sikkerhet (NIS2) setter krav om cybersikkerhet for viktige/kritiske funksjoner
 - GDPR setter krav om beskyttelse av persondata.
 - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (bransjenorm).
- Merk at regelverk og juridiske krav om informasjonssikkerhet ofte henviser til risikovurdering.

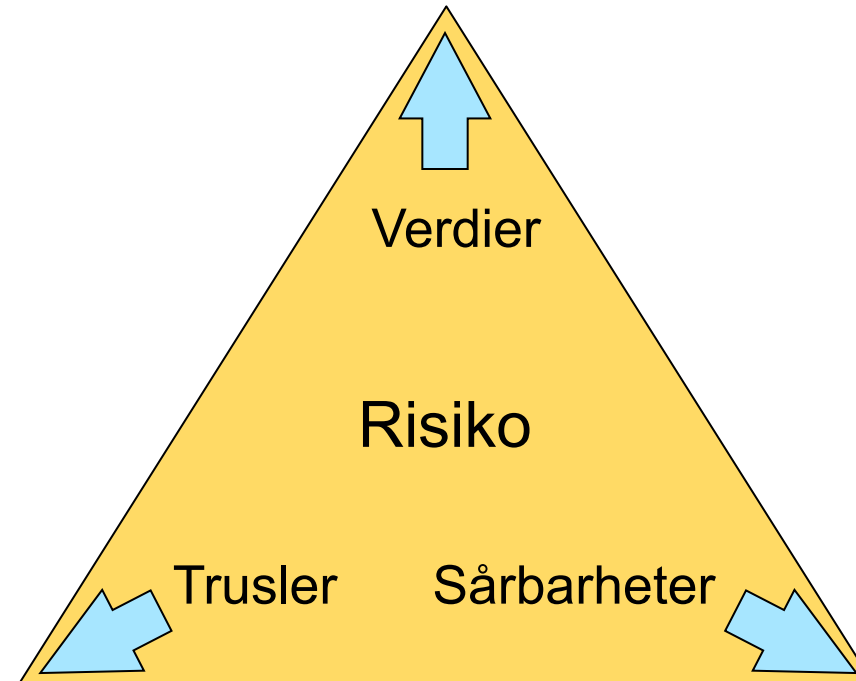


Målsetting for styring av informasjonssikkerhet

- Ville det være mulig å løse alle sikkerhetsproblemer?
- Nei, fordi:
 - Det oppdages stadig nye sårbarheter i gamle systemer
 - Nye digitale tjenester, ofte med sårbarheter, eksponeres online
 - Trusselaktører er flinke til å finne sårbarheter som kan utnyttes
 - Det utvikles stadig mer effektive angrepsverktøy
 - Økende antall og alvorlighet av trusler
- Konklusjon: Informasjonssikkerhet er en kontinuerlig prosess for å stoppe trusler og fjerne sårbarheter
- Målsetting for styring av informasjonssikkerhet er å oppnå god balanse mellom sikkerhetsrisiko og sikkerhetstiltak.



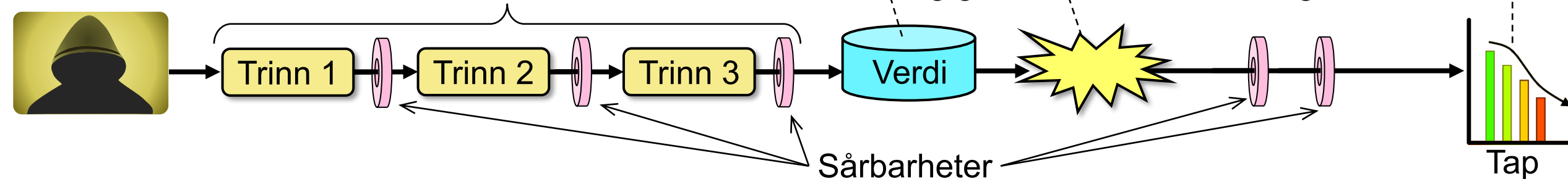
Generell risikomodell for IT-sikkerhet



- Generell modell for risiko
 - Jo større og flere verdier du har, jo større og flere trusler du er utsatt for, og jo mere sårbar du er, desto større risikoeksponering har du.

Verdier, Trusler, Sårbarheter og Tiltak

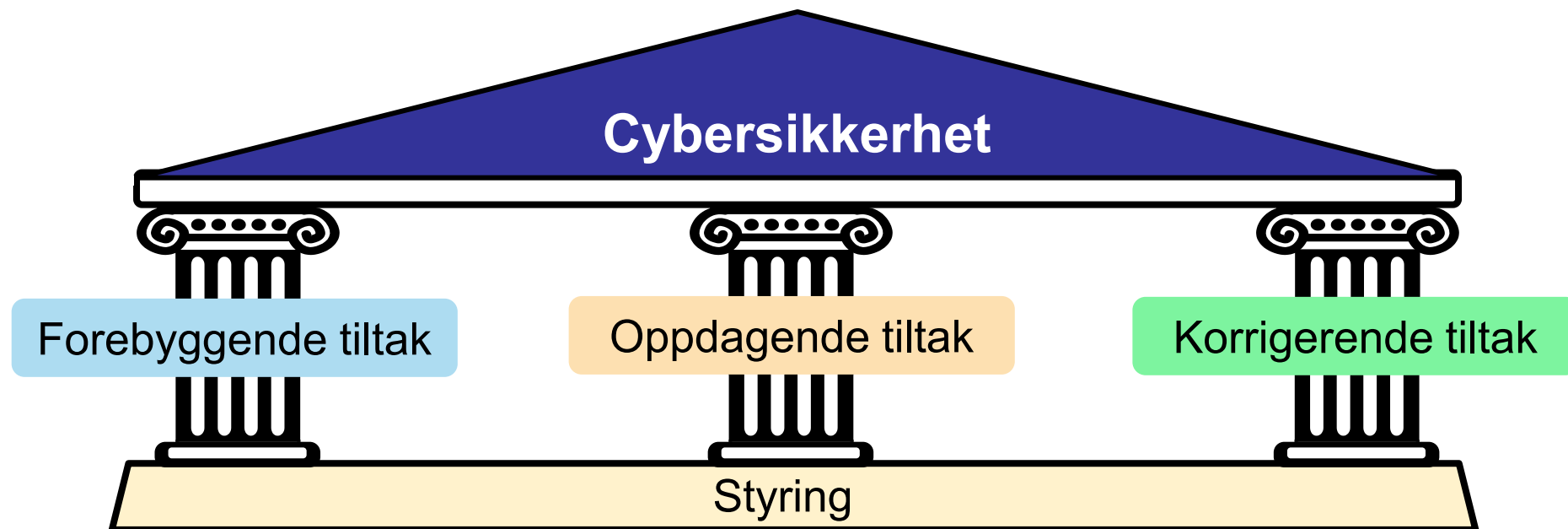
Trusselaktør ... utfører trusselscenario ... som skader verdier og gir hendelse ... med negativ konsekvens



- **Verdier:** Digitale eiendeler som er av verdi for organisasjonen.
 - ENHETER, APPER, NETTVERK, DATA, og BRUKERE
 - Mål for informasjonssikkerhet er å beskytte eiendelenes KIT, avhengig av behov.
 - Person(opplysnings)vern
- **Trussel:** Et potensielt angrepsscenario som kontrolleres av en trusselaktør og som kan skade organisasjonens digitale eiendeler
- **Sårbarhet:** Manglende sikkerhetstiltak mot trusler og evne til å håndtere hendelser.
- **Sikkerhetstiltak** (Security Control): Metode for å forhindre trusler eller redusere konsekvenser av hendelser

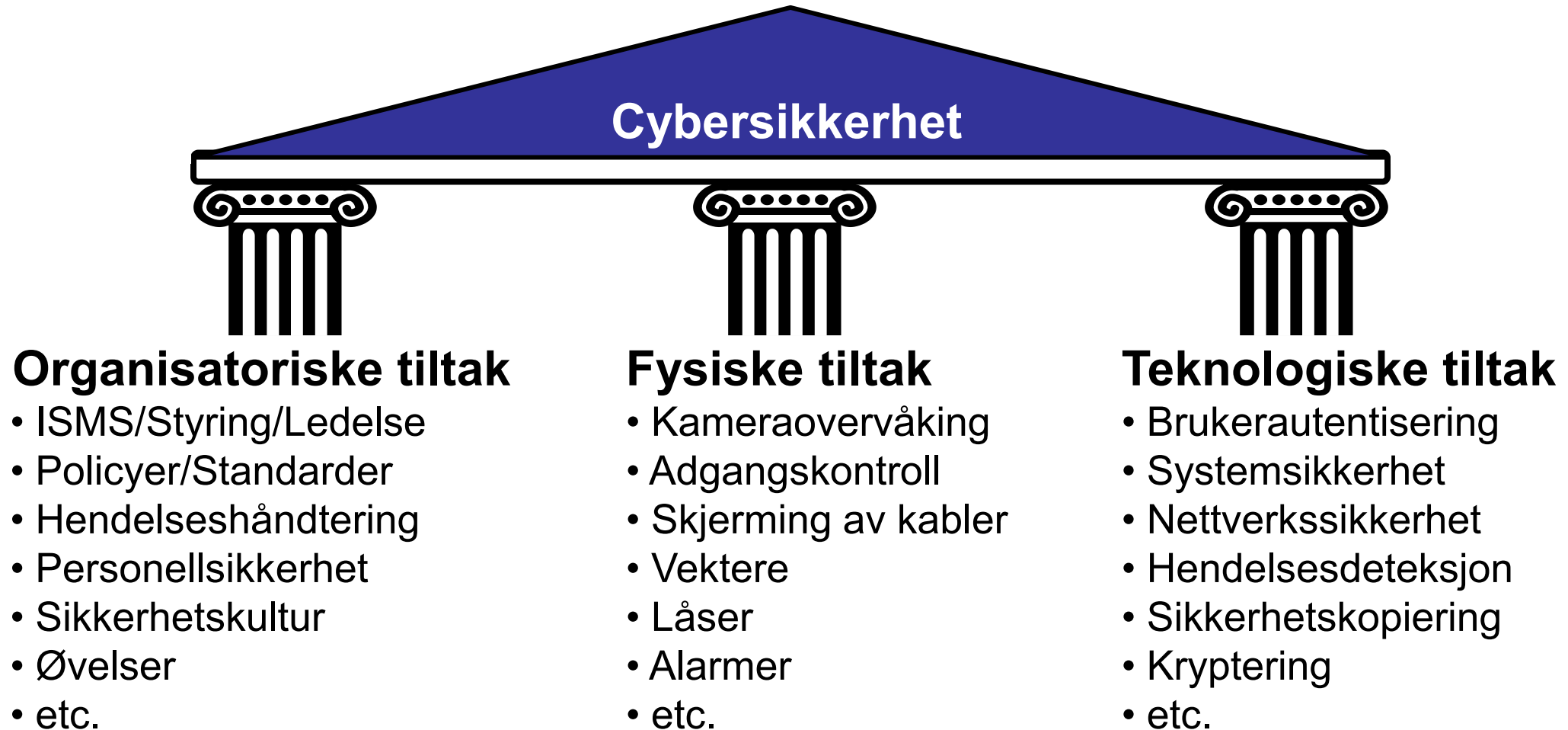
Tiltak for cybersikkerhet

Eksempel kategorisering etter sikkerhetsfunksjoner



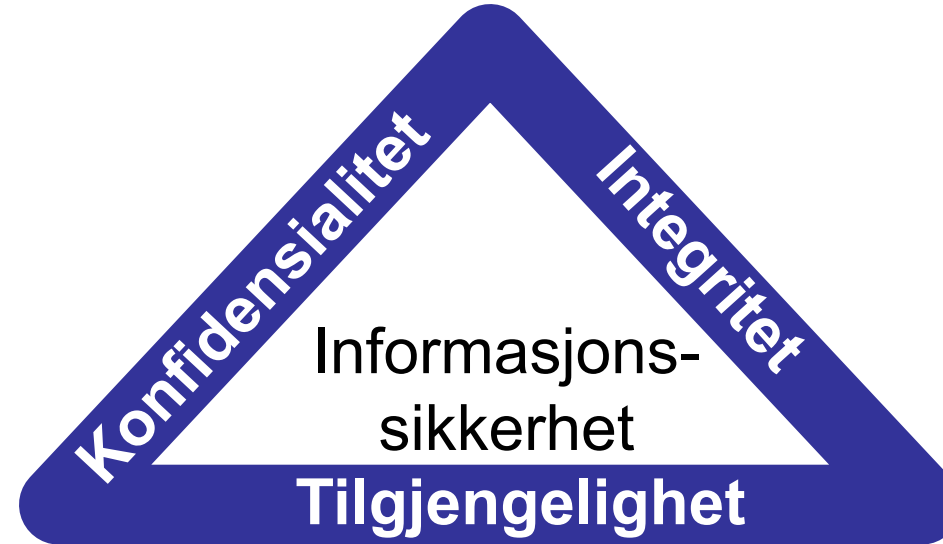
Tiltak for cybersikkerhet

Eksempel kategorisering i tre tematiske domener



Generelle sikkerhetsmål: KIT+P

- Informasjonssikkerhet er tradisjonelt definert som opprettholdelse av KIT.
- Ulike digitale verdier har ulike krav til KIT.
- Engelsk: CIA
 - Confidentiality
 - Integrity
 - Availability:
- Person(opplysnings)vern (data protection) er et tilleggsmål som bl.a. forutsetter KIT. GDPR (General Data Protection Regulation) definerer krav til personvern.



Personvern

Sikkerhetsmål og sikkerhetstiltak

- Sikkerhetsmål
 - Uavhengig av spesifikk implementering
 - Kan implementers med ulike tiltak/controller
- Sikkerhetstiltak / controller / mekanismer
 - Basert på spesifikk implementering, ofte bundet til spesifikke produkter

Sikkerhetsmål:

Konfidensialitet – Integritet – Tilgjengelighet

støtter

Sikkerhetstiltak:

f.eks. låser – kryptering – autentisering - sikkerhetskultur



Analogi for sivil sikkerhet

Konfidensialitet

- Egenskapen av at informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.
(ISO/IEC 27000)
- Trusler:
 - Datatyveri (ekstern trussel)
 - Datalekkasje (intern trussel).
- Sikkerhetstiltak eksempler:
 - Kryptering,
 - Kryptografiske kommunikasjonsprotokoller, f.eks. TLS
 - Autentisering og tilgangskontroll,
 - Anonymisering, f.eks. gjennom pseudonym eller VPN
 - Skallsikring
 - Sikkerhetskultur, bevissthet
 - ...



Integritet

- **Dataintegritet:** Egenskapen av at data ikke har blitt endret eller slettet på en uautorisert måte. (X.800)
- **Systemintegritet:** Egenskapen av å opprettholde korrekthet og kompletthet av dataressurser (ISO/IEC 27000)
- Trusler: Ødelagte data og mis konfigurerte systemer
- Sikkerhetstiltak eksempler:
 - Hashing, MAC, kryptering
 - Konfigurasjonsstyring
 - Endringsledelse
 - Autentisering
 - Tilgangskontroll
 - Sertifisert programvare
 - Sikkerhetskultur, bevissthet
 - ...

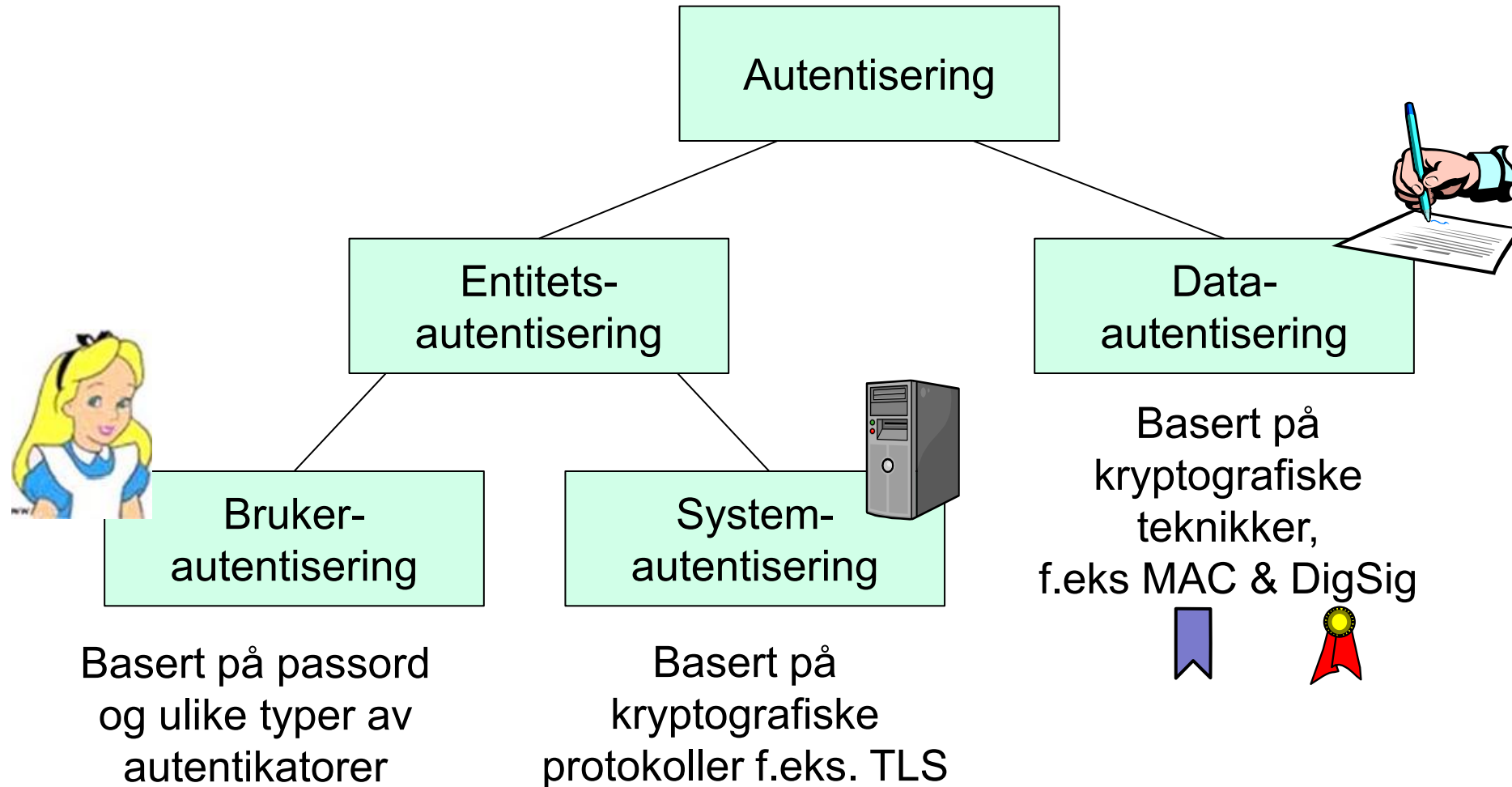


Tilgjengelighet

- Egenskapen av at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet. (ISO/IEC 27000)
- Trusler:
 - Tjenestenekt, overlastangrep (DoS / DDoS)
 - Løsepengevirus
 - Forsinkelse av tidskritiske funksjoner.
- Sikkerhetstiltak eksempler:
 - Redundans av ressurser,
 - Failover-konfigurasjon
 - Brannmur
 - Sikkerhetskopiering (backup)
 - Hendelsesrespons og beredskap,

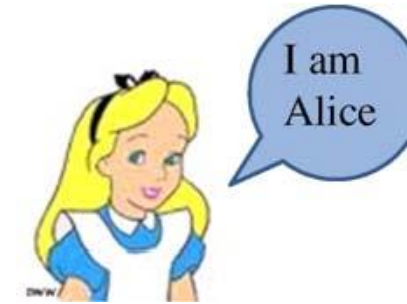


Typer av autentisering

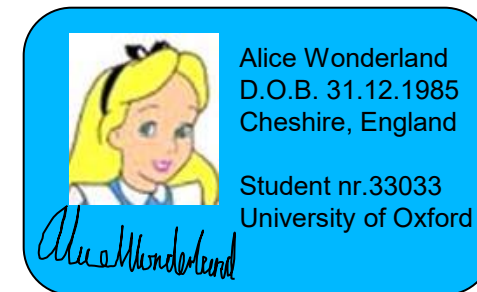


Brukerautentisering

- Oppgi bruker-ID (selv-identifisering)
 - Bruker oppgir (påstår å ha) en bestemt identitet
- Autentisering med autentikator(er)
 - Bevis at du har identiteten du påstår å ha
- Trussel: Identitetstyveri, falsk innlogging
- Sikkerhetstiltak: Autentikatorer, f.eks.:
 - Passord,
 - Personlig kryptografisk brikke,
 - BankID, OTP-generator
 - ID-kort
 - Biometri
 - Sekundære kanaler
 - 2FA, multifaktorautentisering

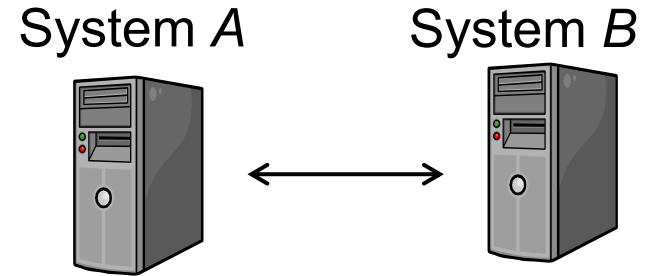


Oppgi bruker-ID



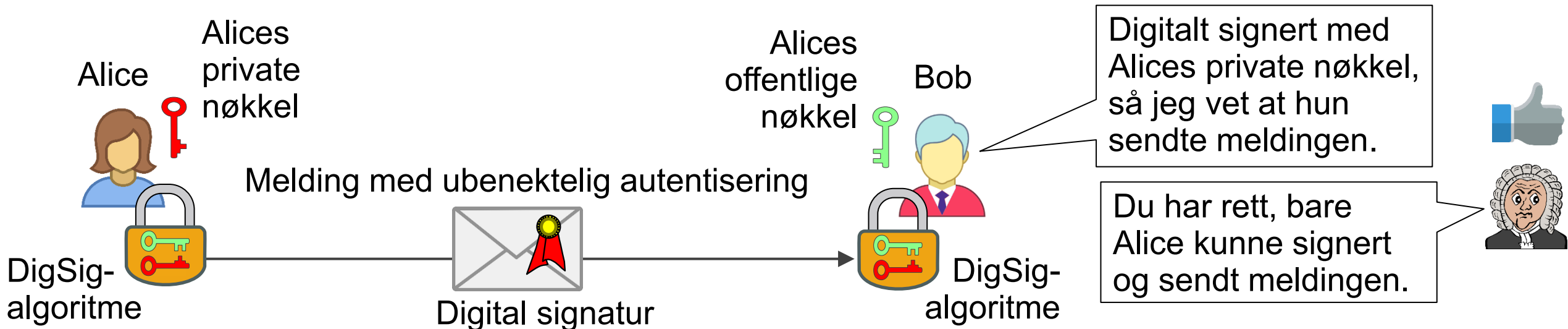
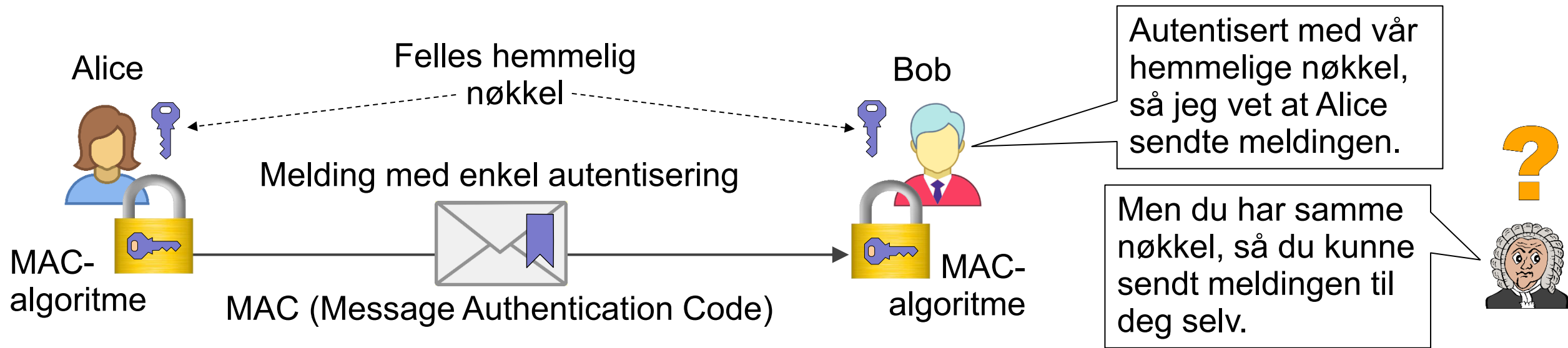
Autentikator for
autentisering

Systemautentisering



- Formål
 - Korrekt identifisering av systemer gjennom nettverk
- Trusler:
 - Falske systemer
 - Falske transaksjoner
 - Man-in-the-middle angrep
 - Nettverksinnbrudd
- Sikkerhetstiltak:
 - Kryptografiske protokoller for autentisering og integritet
 - For eksempel: TLS, IPSEC

Enkel eller ubenektelig meldingsautentisering



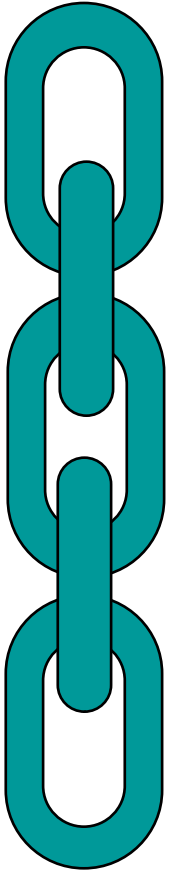
Sporbarhet (Accountability)

- Formål: Å kunne spore hendelser og handlinger til bestemte brukere og entiteter, slik at de må stå til regnskap for sine handlinger (to be accountable)
 - *Logger må oppbevares og beskyttes, slik at handlinger som påvirker sikkerheten kan spores til rette vedkommende.* (TCSEC/Orange Book)
- Trusler:
 - Å ikke være i stand til å identifisere hvem som stod bak en handling
 - Å mangle tilstrekkelig bevis for å kunne gjøre anmeldelse
- Sikkerhetstiltak:
 - Autentisering av alle brukere
 - Logging av systemhendelser
 - Elektroniske bevis
 - Ubenektelighet med digital signatur
 - Digital etterforskning



Pålitelighet

- Egenskapen at systemer ikke inneholder (mange) feil eller svakheter. Hvis feil likevel forekommer, betyr pålitelighet også at systemene kan tolerere visse feil uten at (all) funksjonalitet faller ut.
- Fokuserer mest på å forhindre ikke-tilsiktete hendelser, men er også viktig for å forhindre eller redusere konsekvens av tilsiktete hendelser.
- Trusler:
 - Lav kvalitet i utvikling, konfigurering, feilretting og drift av systemer samt spesielt manglende oppmerksomhet på sikker systemutvikling.
- Tiltak:
 - God (eller beste) praksis for sikker utvikling og drift av systemer, som også kalles «innebygd informasjonssikkerhet»



Tilgangsautorisering



- Tilgangsautorisering er å spesifisere tilgangsrettigheter for entiteter, dvs. for brukere, roller og prosesser
 - Spesifiserer hvem som skal ha tilgang til hva
 - Autoriseringspolicyen er vanligvis definert av mennesker
 - Autoriseringspolicyen blir formalisert som regler og konfigureringer for tilgangskontroll i systemer.
- Autorisering kan bli delegert
 - Leder → Sys.Admin → Bruker
- Vær oppmerksom på forvirring i andre lærebøker og kilder:
 - Noen steder defineres tilgangsautorisering som ekvivalent med tilgangskontroll. Dette er fullstendig feil, fordi den gjør definisjonen på konfidensialitet meningsløs, på den måten at det ikke ville være et brudd på konfidensialitet hvis en hacker får tilgang til en konto med et cracket passord og stjeler data.

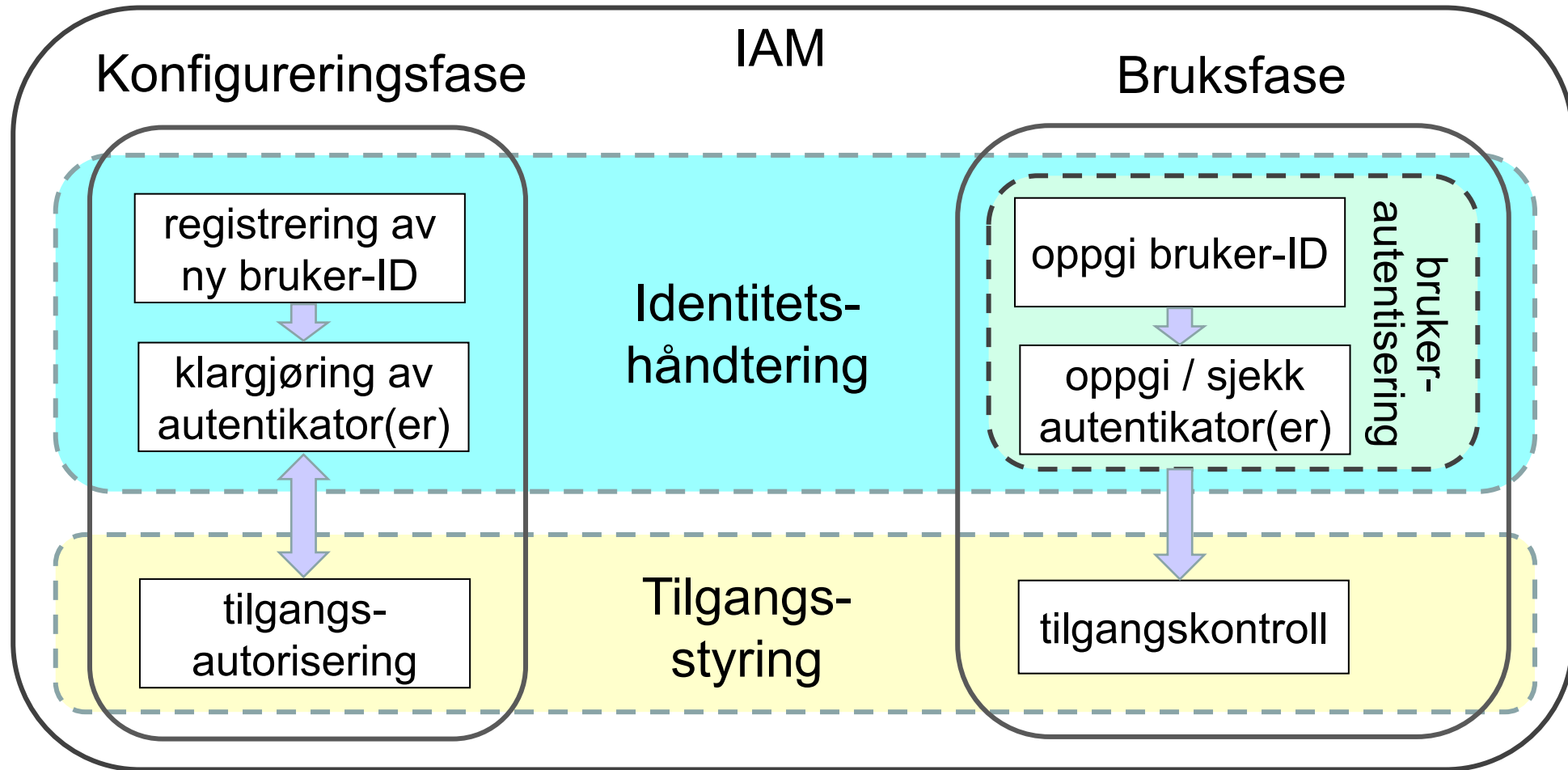
Tilgangskontroll



- Tilgangskontroll foregår etter at brukeren er autentisert.
- Brukeren/entiteten må være autentisert for at systemet skal vite hvem som prøver å utføre en handling eller forespør tilgang.
- Tilgangskontroll benytter autoriseringspolicy/regler for å avgjøre om brukeren er autorisert for tilgang til ressurser.
- Policy/regler for tilgangsautorisering defineres under konfigureringsfasen slik at tilgangskontroll kan utføres under bruksfasen.
- Mange ulike måter å definere regler for tilgangskontroll, f.eks.
 - Identitetsbasert (DAC)
 - Merkebasert (MAC)
 - Rollebasert (RBAC)
 - Attributtbasert (ABAC) (generalisering av alle måtene ovenfor)

Identitetshåndtering og tilgangsstyring

IAM (Identity and Access Management)

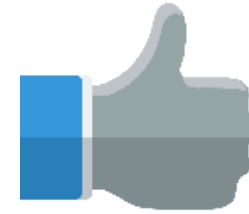


Øversettelse av engelske begreper

Engelsk

Norsk

- | | | |
|-------------------------|--------|------------------------|
| • security/insecurity | —————→ | • sikkerhet/usikkerhet |
| • safety/unsafety | —————→ | • trygghet/utrygghet |
| • certainty/uncertainty | —————→ | • visshet/uvissheit |



*Presis
oversettelse*

- | | | |
|---|----------|------------------------|
| <ul style="list-style-type: none">• security/insecurity• safety/unsafety• certainty/uncertainty | } —————→ | • sikkerhet/usikkerhet |
|---|----------|------------------------|



*Upresis
oversettelse*

Reports

Published: 14 January 2026

Global Risks Report 2026

Download PDF 

The *Global Risks Report 2026*, the 21st edition of this annual report, marks the second half of a turbulent decade. The report analyses global risks through three timeframes to support decision-makers in balancing current crises and longer-term priorities. Chapter 1 presents the findings of this year's **Global Risks Perception Survey (GRPS)**, which captures insights from over 1,300 experts worldwide. It explores risks in the current or immediate term (in 2026), the short-to-medium term (to 2028) and in the long term (to 2036). Chapter 2 explores the range of implications of these risks and their interconnections, through six in-depth analyses of selected themes. Below are the key findings of the report, in which we compare the risk outlooks across the three-time horizons.



Short term (2 years)

1. Geoeconomic confrontation
2. Misinformation and disinformation
3. Societal polarization
4. Extreme weather events
5. State-based armed conflict
6. Cyber insecurity
7. Inequality
8. Erosion of human rights and/or of civic freedoms
9. Pollution
10. Involuntary migration or displacement

- Cyberusikkerhet (dvs. utilstrekkelig beskyttelse av digitale verdier mot skade) rangeres som den 6. største risiko for verdensøkonomien, etter væpnede konflikter mellom stater på 5. plass.

Slutt på presentasjonen

